UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,179	12/02/2003	Simon Robert Walmsley	PEA16US	5306

24011 7590 09/17/2008
SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER	
HOANG, DANIEL L	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
09/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/727,179	**Applicant(s)** WALMSLEY ET AL.
	Examiner DANIEL L. HOANG	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _04 June 2008_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-10_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-10_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 6/04/08 have been fully considered but they are not persuasive. Applicant argues that the cited reference does not teach that the secret information is not stored by the non-volatile memory. Applicant alleges that instead of not storing the secret information, Hameau specifically discloses that the random number NAC is stored by the smart card. Examiner respectfully disagrees. The cited passage in the Hameau reference, paragraph 50, teaches that the random number is retrieved from the smart card. The random number is generated by the computing means of the smart card. Hameau does not disclose that this random number is stored on the card. The fact that this number is random and is computed clearly shows that it is generated when requested and does not need to be stored on the card. Furthermore, for security reasons, it would be disadvantageous to store the random number. Applicant's arguments are therefore not persuasive and the previous action's rejections are maintained.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The claim cites secret information not being stored by the non-volatile memory. Examiner is unable to find support for this limitation in applicant’s specification. Appropriate correction is required.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3, 5-8, and 10 are rejected under 35 U.S.C. 102(e) as being anticipated by Hameau et al., US PGP No. 20020107798.

As per claim 1:

Hameau teaches:

An integrated circuit comprising a processor and non-volatile memory, the non-volatile memory storing a first number and a second number, wherein the second number is the result of an encryption function taking a third number and secret information as operands, the secret information not being stored by the non-volatile memory and the integrated circuit comprising software configured to decrypt the second number using the first number, thereby to determine the secret information as required.

> *[see paragraph 8] "Written into a nonvolatile part of the aforementioned storage means of the microchip, in permanent (using "Read Only Memory" or "ROM"), or semi-permanent ("Electrically Erasable Programmable Read Only Memory" or "EEPROM") fashion, is so-called secret data required for these functions: encryption algorithm, secret encryption keys, identification data, etc."*
>
> *[see paragraph 50] "As shown in FIG. 2, using an outgoing order O.sub.s, the "SAM" 3 retrieves from the smart card CP a sixteen-byte random number N.sub.aC. The number N.sub.aC will hereinafter be called the "card random number," and can be generated, for example, by the computing means of the smart card CP, in the example illustrated a microprocessor CPU. The "SAM" 3 also generates a sixteen-byte random number that will be called the "SAM random number" N.sub.aS."*
>
> *[see paragraph 58] "From the secret master key K.sub.M and from the aforementioned sixteen-byte random number N.sub.aC, the smart card CP generates a sixteen-byte symmetric, secret*

> *so-called session key K.sub.S, making it possible to calculate a cryptogram specific to the smart card CP."*
>
> *[see paragraph 66] "The "SAM" 3 is capable of calculating the same secret session key K.sub.S in the manner just described, since the latter also stores the secret master key K.sub.M."*

As is evident in the citations above, the smart card comprising a microchip is interpreted as the claimed "integrated circuit comprising a memory." As is also cited, the nonvolatile part of the smart card stores secret data. The master key of the smart card is being interpreted as the claimed "first number". The master key of the SAM is being interpreted as the claimed "third number". The sixteen byte random number is being interpreted as the claimed "secret information". The secret session key that is generated using the secret master key and the sixteen byte random number is interpreted as the claimed "second number". As is consistent with the claim, the secret session key is the result of an encryption function taking the master key and the sixteen byte random number as the operands. As can be seen in paragraphs 25 and 26 of the reference, the smart card can derive the secret information sent from the SAM by using its own copy of the master key.

As per claim 2, Hameau teaches:

An integrated circuit according to claim 1, wherein the first and third numbers are the same.

> *[see paragraph 23] "storage means of said microchip storing a symmetric secret encryption key and an asymmetric public key and said security device storing the same symmetric secret encryption key."*

As per claim 3, Hameau teaches:

An integrated circuit according to claim 1, wherein the first and second numbers are of the same length.

> *[see rejection of claim 2, wherein both are the same and thus clearly are the same length.]*

As per claim 5, Hameau teaches:

An integrated circuit according to claim 1, wherein the encryption function is an XOR logical function.

> *[see paragraph 63] “The part K.sub.S1 is re-injected through a first input of a logic circuit of the "exclusive-OR" type, referenced XOR.”*

As per claim 6, Hameau teaches:

An integrated circuit according to claim 5, wherein the software is configured to decrypt the second number by performing an XOR logical function using the first and second numbers as operands.

> *[see paragraph 65] “the "exclusive-OR" logic operation can be performed by means of software instead of using a specific logic circuit XOR, by calling a routine stored in "ROM" memory 1, for example, under the control of the microprocessor CPU.”*

As per claim 7, Hameau teaches:

A method of manufacturing a plurality of integrated circuits in accordance with claim 1, including the steps, for each integrated circuit, of: determining the first number, the third number and the secret information; generating the second number by way of an encryption function that uses the third number and the secret information as operands; storing the first and second numbers on the integrated circuit.

> *[see paragraph 80] “The method makes it possible to load, into each smart card CP, its own key, or in other words a different key than the other smart cards.*

As per claim 8, Hameau teaches:

A method according to claim 7, wherein the first number is different amongst at least a plurality of the integrated circuits.

> *[see rejection of claim 7 wherein each smart card is loaded with its own keys]*

As per claim 10, Hameau teaches:

A method according to claim 7, wherein the first number is stored on the integrated circuit first, then extracted therefrom for use in generating the third and thence the second number.

> *[see rejection of claim 1, wherein the master key is stored on the smart card and then used to derive the remaining security data]*

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hameau as applied to claim 1 above, and further in view of Pires (US Patent No. 6,269,164.

As per claim 4:

An integrated number according to claim 1, wherein the first number is a random number that was generated using a stochastic process.

> *The Hameau reference has been discussed above. Hameau does not expressly disclose that the first number is a random number that is generated using a stochastic process. Pres teaches of a stochastic key.*
>
> *[see col. 18, lines 2-7] "stochastic key scrambling method previously described is particularly well suited to the creation of good keys. As stated before, a good key is one made by a process that distributes the keys it generates evenly over the entirety of the available key space regardless of the input used to create it."*

It would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to modify the Hameau reference to incorporate the teachings of Pires in order to include usage of a random key generated using a stochastic process in order to improve upon the security of the key and to generate a key that is difficult to obtain because it is created through a random process.

As per claim 9, Hameau teaches:

A method according to claim 8, wherein the first numbers are determined randomly, pseudo-randomly, or arbitrarily.

[see rejection of claim4 wherein a stochastic process leads to randomness]

CONCLUSION

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/
Examiner, Art Unit 2136

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136